SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

OCT 18 2012

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Deterring and Preventing Unauthorized Disclosures of Classified Information

Unauthorized disclosures of classified information put at risk the success of the most sensitive classified operations, plans, partnerships, and technologies of DoD and our mission partners. It is not an overstatement to say that human lives are at times jeopardized when someone leaks classified information. We can and must do a better job of deterring and preventing these types of disclosures. Towards this end:

- In addition to the requirements currently in place (including those in DoD Directive 5210.50, DoD Instruction 5200.01, and DoD Manual 5200.01), I am directing a "top down" approach to improve the identification, investigation, and reporting of unauthorized disclosures of classified information. The Assistant to the Secretary of Defense for Public Affairs, in consultation with the Under Secretary of Defense for Intelligence (USD(I)), will review all major, national media reporting for unauthorized disclosures of DoD classified information. USD(I) will then ensure that the appropriate component of the Department is tasked with investigating leaks and, when appropriate, initiating the process for appropriate referrals to the Department of Justice.

- USD(I), in consultation with the Assistant Secretary of Defense for Legislative Affairs, will ensure prompt and complete reporting to Congress of all incidents that the law requires to be reported under 10 U.S.C. § 2723.

- To further strengthen accountability in our reporting system, all DoD Components shall use the central DoD-wide security incident reporting system established by USD(I), in addition to existing reporting requirements. I expect DoD Components to ensure all incidents are promptly reported and appropriately classified to comply with the attached USD(I) memorandum, dated June 19, 2012. The OUSD(I) Security Directorate will be the Department's central office to monitor and ensure the prompt reporting, investigation, and referral of unauthorized disclosures of classified information to the Department of Justice and notifications to Congress.

- I hereby reiterate the guidance provided in DoD Directive 5122.05 that the Assistant to the Secretary of Defense for Public Affairs is the sole release authority to news media for official DoD information, as defined by DoD Directive 5230.09. All media inquiries must be coordinated through appropriate public affairs channels.

- In coordination with the Office of the DoD General Counsel, I expect all DoD Components to continue to cooperate fully in the pending leak investigations by the United States Attorneys for the District of Maryland and the District of Columbia.

In addition, the Department, in collaboration with the Director of National Intelligence, is finalizing a strategic plan to address unauthorized disclosures. This plan will integrate and strengthen the Department's processes to report, investigate, assess damage, and monitor implementation of administrative, management, and investigative actions. It will harmonize the processes used within DoD and the Intelligence Community to ensure that gaps in effective controls and oversight are closed.

I expect each of you to exert your leadership to drive this message throughout your respective organizations, as well as to enforce my direction that such incidents will be appropriately reported and investigated and that all DoD personnel cooperate fully and support such investigations. I expect your personal engagement in reviewing, developing, and implementing your own policies and procedures to prevent, report, and investigate unauthorized disclosures of classified information thoroughly, promptly, and vigorously.

I am committed to implementing a comprehensive solution that drives change in the culture and the attitude about leaking classified information. Personnel who disclose classified information without authorization, in addition to having potentially committed a crime, breach the trust that we, as leaders, have placed in them. As senior leaders in the Department, we are responsible for ensuring our personnel remain true to their oath to "well and faithfully discharge" their duties as Federal employees and members of the Armed Forces of the United States. Your personal engagement, aggressive implementation of the unauthorized disclosures strategic plan, and prompt reporting are essential to protecting DoD personnel, information, operations and infrastructure. The OUSD(I) point of contact is Ms. Theresa Ramsey, who can be reached at 703-604-1116 or Theresa.Ramsey@osd.mil.

Attachment:
As stated

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINSTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

JUN 19 2012

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Improving Policy and Procedures for Unauthorized Disclosure Reporting

Unauthorized disclosures of classified national security information represent a failure to properly protect critical DoD operations and resources. Unfortunately, we continue to see an increase in the number of unauthorized disclosures as well as an increase in the sensitivity of the information disclosed. As the Principal Staff Assistant for DoD security, I am directing a series of actions to strengthen oversight, compliance, and accountability.

Consistent with the WikiLeaks Task Force recommendations, I am directing the use of a DoD-wide security incident reporting mechanism. Effective immediately, all DoD component security managers shall begin reporting incidents of unauthorized disclosures of classified information using the Security Incident Report (SIR), an internal module of the Operations Security Collaboration Architecture (OSCAR). The SIR gathers all mandatory elements of an unauthorized disclosure report described in Enclosure 6 of DoD Manual 5200.01, Volume 3. Security managers who have not already done so must establish an OSCAR account and specifically request access to the SIR module. Instructions on how to do so may be obtained from the point of contact named below.

Also, I have established a cross-functional working group to develop a comprehensive plan of action and milestones. This group will collaborate with a similar effort by the Office of the Director of National Intelligence designed to deter unauthorized disclosures of classified information, encourage reporting of systemic security vulnerabilities, and mitigate the risk to national security information and resources. The point of contact is Mr. Ed Kaufhold at (703) 604-1222 or edmund.kaufhold@osd.mil.

Michael G. Vickers

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES